

CLAIMS

What is claimed is:

1. A method of providing a circle of trust comprising:

receiving a first certificate of a first affiliated entity by a second affiliated entity;

5 storing said first certificate of said first affiliated entity in a first trusted partner

list accessible by said second affiliated entity;

receiving a second certificate of said second affiliated entity by said first affiliated entity; and

storing said second certificate of said second affiliated entity in a second trusted

10 partner list accessible by said second affiliated entity;

wherein access to a resource is controlled as a function of said first trusted partner list or said second trusted partner list.

2. The method according to Claim 1 further comprising:

15 initiating use of a resource on a relying party device by a client device, wherein an authentication assertion reference is provided by a client device;

determining an identity of an issuing party as a function of said authentication assertion reference;

sending an authentication request containing a certificate of said relying party to

20 said issuing party;

determining if said certificate is contained in a trusted partner list of said issuing party;

sending an authentication assertion, indicating that said client has been authenticated, from said issuing party to said relying party when said certificate is contained in a trusted partner list of said issuing party;

5 sending an authentication assertion, indicating that said client has not been authenticated, from said issuing party to said relying party when said certificate is not contained in said trusted partner list of said issuing party; and

providing said requested resource to said client device by said relying party when said authentication assertion indicates that said client has been authenticated.

10 3. The method according to Claim 2, further comprising:
logging-on to said issuing party utilizing said client device; and
authenticating said client device by said issuing party.

15 4. The method according to Claim 1, further comprising:
receiving a first network address of said first affiliated entity by said second affiliated entity;
storing said first network address of said first affiliated entity in said first trusted partner list accessible by said second affiliated entity;
receiving a second network address of said second affiliated entity by said first
20 affiliated entity; and
storing said second network address of said second affiliated entity in said second trusted partner list accessible by said second affiliated entity.

5. The method according to Claim 4, further comprising:

initiating user of a resource on a relying party device by a client device, wherein an authentication assertion reference is provided by a client device;

determining an identity of an issuing party as a function of said authentication
5 assertion reference;

sending an authentication request from a relying party to an issuing party;

determining a network address of said relying party from said authentication
request;

determining if said network address is contained in a trusted partner list of said
10 issuing party;

sending an authentication assertion, indicating that said client has been
authenticated, from said issuing party to said relying party when said network address is
contained in a trusted partner list of said issuing party;

sending an authentication assertion, indicating that said client has not been
15 authenticated, from said issuing party to said relying party when said network address is
not contained in said trusted partner list of said issuing party; and

providing said requested resource to said client device by said relying party when
said authentication assertion indicates that said client has been authenticated.

20 6. The method according to Claim 4, wherein said first network address and said
second network address comprises a first and second internet protocol (IP) address
respectively.

7. The method according to Claim 1, further comprising:

receiving a first network address of a third affiliated entity by said first affiliated entity;

storing said first network address of said third affiliate entity in said second
5 trusted partner list accessible by said first affiliated entity;

receiving a second network address of said first affiliated entity by said third affiliated entity; and

storing said second network address of said first affiliated entity in a third trusted partner list accessible by said third affiliated entity.

10

8. A method of providing a circle of trust comprising:

initiating user of a resource on a relying party device by a client device, wherein an authentication assertion reference is provided by a client device;

determining an identity of an issuing party as a function of said authentication
15 assertion reference;

sending an authentication request containing a certificate of said relying party to said issuing party;

determining if said certificate is contained in a trusted partner list of said issuing party;

20 sending an authentication assertion, indicating that said client has been authenticated, from said issuing party to said relying party when said certificate is contained in a trusted partner list of said issuing party;

sending an authentication assertion, indicating that said client has not been authenticated, from said issuing party to said relying party when said certificate is not contained in said trusted partner list of said issuing party; and

providing said requested resource to said client device by said relying party when
5 said authentication assertion indicates that said client has been authenticated.

9. The method according to Claim 8, further comprising:

sending an authentication request from said relying party to said issuing party;

determining a network address of said relying party from said authentication
10 request;

determining if said network address is contained in a trusted partner list of said issuing party;

sending an authentication assertion, indicating that said client has been authenticated, from said issuing party to said relying party when said network address is
15 contained in a trusted partner list of said issuing party;

sending an authentication assertion, indicating that said client has not been authenticated, from said issuing party to said relying party when said network address is not contained in said trusted partner list of said issuing party; and

providing said requested resource to said client device by said relying party when
20 said authentication assertion indicates that said client has been authenticated.

10. The method according to Claim 9, wherein said first network address and said second network address comprise a first and second internet protocol (IP) address respectively.

5 11. The method according to Claim 8, further comprising:
logging-on to an issuing party utilizing said client device; and
authenticating said client device by said issuing party.

12. A system for providing a circle of trust comprising:
10 a first affiliated entity comprising;
 a first administration module; and
 a first trusted partner list communicatively coupled to said first administration module; and
said second affiliated entity comprising;
15 a second administration module; and
 a second trusted partner list communicatively coupled to said second administration module.

13. The system for providing a circle of trust according to Claim 12, wherein said
20 first administration module receives said credential of said second affiliated entity.

14. The system for providing a circle of trust according to Claim 13, wherein said first administration module stores said credential of said second affiliated entity in a trusted partner list.

5 15. The system for providing a circle of trust according to Claim 14, wherein said credential comprises a certificate.

16. The system for providing a circle of trust according to Claim 14, wherein said credential comprises a network address.

10

17. The system for providing a circle of trust according to Claim 13, further comprising:

a client device;

a first affiliated entity communicatively coupled to said client device and a second
15 affiliated entity, comprising;

a first session module; and

a first authentication module; and

said second affiliated entity communicatively coupled to said client device and
said first affiliated entity, comprising;

20 a second session module; and

a second trusted partner list.

18. The system for providing a circle of trust according to Claim 17, wherein said second session module determines the identity of an issuing party as a function of an authentication assertion reference received from said client device.

5 19. The system for providing a circle of trust according to Claim 17, wherein said first session module determines a trusted status of said second affiliated entity as a function of a certificate received from said second session module.

10 20. The system for providing a circle of trust according to Claim 17, wherein said first session module determines a trusted status of said second affiliated entity as a function of a network address of said second session module.

21. A system for providing a circle of trust comprising:
a client device;
15 a first affiliated entity communicatively coupled to said client device and a second affiliated entity, comprising;
a first session module; and
a first authentication module; and
said second affiliated entity communicatively coupled to said client device and
20 said first affiliated entity, comprising;
a second session module; and
a second trusted partner list.

22. The system for providing a circle of trust according to Claim 21, wherein said first session module provides for secure transfer of information for authenticating a user on said client device.

5 23. The system for providing a circle of trust according to Claim 22, wherein said first session module generates and processes SAML requests and assertions contained in SOAP envelopes.

24. The system for providing a circle of trust according to Claim 21, wherein said
10 second session module determines the identity of an issuing party as a function of an authentication assertion reference received from said client device.

25. The system for providing a circle of trust according to Claim 21, wherein said first session module determines a trusted status of said second affiliated entity as a
15 function of a certificate received from said second session module.

26. The system for providing a circle of trust according to Claim 21, wherein said first session module determines a trusted status of said second affiliated entity as a function of a network address of said second session module.
20

27. The system for providing a circle of trust according to Claim 21, wherein said first session module determines said network address of said session module from an HTTP header.

28. A computer readable-medium containing a plurality of instructions which when executed cause a network device to implement a method of providing a circle of trust comprising:

5 receiving a first network address of a first affiliated entity by a second affiliated entity;

 storing said first network address of said first affiliated entity in a first trusted partner list accessible by said second affiliated entity;

 receiving a second network address of said second affiliated entity by said first
10 affiliated entity; and

 storing said second network address of said second affiliated entity in a second trusted partner list accessible by said second affiliated entity.

29. The computer readable-medium according to Claim 28, further comprising
15 initiating use of a resource on a relying party device by a client device, wherein an authentication assertion reference is provided by a client device;

 determining an identity of an issuing party as a function of said authentication assertion reference;

 sending an authentication request from a relying party to an issuing party;

20 determining a network address of said relying party from said authentication request;

 determining if said network address is contained in a trusted partner list of said issuing party;

sending an authentication assertion, indicating that said client has been authenticated, from said issuing party to said relying party when said network address is contained in a trusted partner list of said issuing party;

5 sending an authentication assertion, indicating that said client has not been authenticated, from said issuing party to said relying party when said network address is not contained in said trusted partner list of said issuing party; and

providing said requested resource to said client device by said relying party when said authentication assertion indicates that said client has been authenticated.

10 30. The computer readable-medium according to Claim 28, further comprising:
receiving a first certificate of a first affiliated entity by a second affiliated entity;
storing said first certificate of said first affiliated entity in said first trusted partner list accessible by said second affiliated entity;

15 receiving a second certificate of said second affiliated entity by said first affiliated entity; and

storing said second certificate of said second affiliated entity in said second trusted partner list accessible by said second affiliated entity.

20 31. The computer readable-medium according to Claim 30, further comprising:
sending an authentication request containing a certificate of said relying party to said issuing party;

determining if said certificate is contained in a trusted partner list of said issuing party;

sending an authentication assertion, indicating that said client has been authenticated, from said issuing party to said relying party when said certificate is contained in said trusted partner list of said issuing party;

5 sending an authentication assertion, indicating that said client has not been authenticated, from said issuing party to said relying party when said certificate is not contained in said trusted partner list of said issuing party; and

providing said requested resource to said client device by said relying party when said authentication assertion indicates that said client has been authenticated.

10 32. The computer readable-medium according to Claim 31, further comprising:
logging-on to said issuing party utilizing said client device; and
authenticating said client device by said issuing party.